



Wer hört hier mit? Fast jeder, wenn er das will.

[Reuters]

Handy-Abhören für jedermann

Tagung. Experten zeigen massive Sicherheitslücken auf, die mit wenig Geschick und Geld von jedermann angreifbar sind. Spionagesoftware ist indes schon ab 35 Euro zu haben.

VON ANDREAS WETZ

[WIEN] Damals, als Ex-Finanzminister Karl-Heinz Grasser, der Lobbyist Walter Meischberger und der Immobilienmakler Ernst Karl Plech ihre inzwischen legendären Telefonate führten, wähten sie sich sicher. Der Einsatz nicht registrierter Prepaid-Handys und die Verschlüsselung des GSM-Mobilfunks sollten reichen. Tat es aber nicht. Die Polizei stand mit einem 500.000 Euro teuren Spezialgerät vor der Tür und hörte mit.

Das war im Februar 2010. Heute, eineinhalb Jahre später, ist so etwas auch für interessierte Laien möglich, bald vermutlich für jedermann. So lautet die Botschaft einer Fachtagung zum Thema Sicherheit in Kommunikations- und Informationstechnologie in Wien. Veranstalter ist das Abwehramt, der Inlandsnachrichtendienst des Bundesheeres, der im Zuge des Treffens Spitzenkräfte aus den Bereichen Wirtschaft, Exekutive und Militär zum Wissensaustausch über neue Entwicklungen und Bedrohungen lud.

Zentrale Erkenntnis: Die rasend schnell voranschreitende Verbreitung von Smartphones wird zur Bedrohung für Staat, Wirtschaft und jeden Bürger. Ein Mitarbeiter des Bundesamts für Verfassungsschutz und Terrorismusbekämpfung (BVT) drückt es so aus: „Wer Zugriff auf das Smartphone eines Dritten erlangt, übernimmt dessen Leben.“ Die Geräte „wissen“ alles, weil sie buchstäblich und immer hautnah an ihren Besitzern sind, speichern Bewegungsprofile, E-Mails, SMS, Kommunikationsverhalten, Termine, Bekanntenkreis, Fotos, Videos und noch viel mehr.

Mehrere dubiose Entwickler – oftmals aus dem fernen Osten – bieten inzwischen ganze Spionagepakete zum Diskontpreis an. 24-Stunden-Support via E-Mail inklusive. Für 59,95 US-Dollar (44 Euro) erhält man etwa die Software „Cell Spy“. Sie muss per Datenkabel, oder besser unbemerkt via WLAN, am Telefon installiert werden. Ob iPhone, Android-Betriebssystem oder Blackberry spielt dabei keine Rolle. Danach besitzt

man Fernzugriff auf Kontaktlisten, SMS-Speicher und die Telefonfunktion. Im „Presse“-Test funktionierte auch das wohl bedenklichste Feature auf Anhieb: Ein Anruf beim infizierten Handy verwandelt dieses in eine mobile Wanze. Ohne dass der Betroffene das Gespräch annehmen muss, ohne jegliche Reaktion am Display, können eine Verbindung aufgebaut und das Mikrofon aktiviert werden. So ist es möglich, über ein gekapertes Mobiltelefon vom anderen Ende der Welt aus die Ehefrau zu belauschen. Oder jemand anderen.

Industriespionage boomt

„Haupteinsatzzweck solcher Methoden ist Industriespionage“, sagt Marco Di Filippo vom schweizerischen Sicherheitsdienstleister Compass. Eine Studie des BVT und der FH Campus Wien bestätigt das. Die Autoren gehen davon aus, dass fast jedes dritte Unternehmen bereits Opfer eines „ungewollten Informationsabflusses“ wurde. Di Filippo: „Dabei hat das Abhören von Handys das Potenzial, zum Volkssport zu werden.“

Für interessierte Laien ist das schon heute keine Schwierigkeit mehr. In diesen Kreisen einen fast legendären Ruf hat ein altes Handy des Herstellers Motorola. Das Modell C123 ist gebraucht ab etwa zehn Euro zu haben. Kauft man für weitere 25 Euro ein passendes Datenkabel und lädt die kostenfreie Software „OsmocomBB“ aus dem Internet, sind alle Handy-Telefonate, die aktuell über denselben Sendemasten laufen, mitzuhören. Darüber hinaus gibt es das – ebenfalls frei – Programm OpenBTS, mit dem Interessierte ihren eigenen GSM-Sender betreiben können, den sie dann – wie einst die Polizei bei Grasser – in der Nähe des Wohnorts ihres Opfers aufstellen. Die nötige Hardware kostet als Selbstbausatz und je nach Qualität zwischen 150 und 900 Euro.

Der Einsatz dieser Methoden ist strafbar. Die Berichte von BVT und den Heeresdiensten zeigen jedoch, dass sie immer öfter zum Einsatz kommen. „Das Problem ist, dass Mobiltelefonie aus dem Alltag nicht mehr wegzudenken ist“, so ein Militär zur „Presse“.

Wie Polizei und Nachrichtendienste mithören

Technik. Ein sogenannter IMSI-Catcher blamierte einst Karl-Heinz Grasser & Co. Weltweit gibt es nur eine Handvoll Produzenten der bis zu 500.000 Euro teuren Geräte. Dennoch gilt die Technik als Exportschlager.

[WIEN/AWE] Die Unterhaltung der beiden über die Herkunft einer Provision wurde zum geflügelten Wort. Aufgezeichnet hat die Polizei die Telefonate mit einem IMSI-Catcher (IMSI ist die Seriennummer einer GSM- oder UMTS-SIM-Karte). Diese Geräte werden weltweit von Polizei und Nachrichtendiensten eingesetzt. Vereinfacht gesagt gibt sich ein IMSI-Catcher gegenüber Mobiltelefonen als Sendestation aus, zieht Gespräche auf sich und leitet sie weiter. Gegenüber dem „echten“ Netzwerk täuscht das Gerät vor ein Mobiltelefon zu sein. So können Handys im Sendebereich des IMSI-Catchers abgehört und geortet werden.



Ex-Minister Grasser, von der Polizei beim Telefonieren abgehört.

[EPA]

Je nach Ausstattung und Funktionsumfang des Catchers kostet ein Gerät zwischen 50.000 (nur Ortung) und 500.000 Euro. Hersteller gibt es weltweit nur eine Handvoll, im deutschsprachigen Raum etwa die Firmen Rohde & Schwarz und Neosoft. Trotz der hohen Preise

entwickelte sich die Technik in den vergangenen Jahren zum Exportschlager. Weltweit seien laut Firmeninterna weit über 1000 Geräte im Einsatz.

Verkauft und exportiert werde ausschließlich unter strengen Auflagen. Wie die zuständigen Behör-

den die Geräte einsetzen, gibt immer wieder Anlass für Kritik, denn: In Österreich etwa darf die Polizei die Geräte ohne richterliche Kontrolle nur zur Ortung einsetzen, könnte auf die Abhörfunktion also verzichten. Eben das geschieht am einfachsten – und nur auf richterliche Anordnung – direkt in der Zentrale des Providers. Oppositionspolitiker warnten in der Vergangenheit davor, dass die Behörden zur Umgehung der Kontrolle durch ein Gericht unerlaubt die Abhörfunktion von IMSI-Catchern nutzen könnten. Das Innenministerium dementierte stets. Technisch nachzuweisen wäre ein solcher Missbrauch jedenfalls nicht.